Remarks

Reconsideration of this Application is respectfully requested.

Upon entry of the foregoing amendment, claims 1-24 are pending in the application, with claims 1 and 10 being the independent claims. No new claims are sought to be added. Claims 1, 2, 7-10, 13-15, 18, and 22 are sought to be amended. These changes are believed to introduce no new matter, and their entry is respectfully requested.

Based on the above amendment and the following remarks, Applicant respectfully requests that the Examiner reconsider all outstanding objections and rejections and that they be withdrawn.

Double Patenting

Claims 1, 4-10, 12-17, and 19-22 have apparently been provisionally rejected under 35 U.S.C. 101 on the grounds of statutory type double patenting as being unpatentable over claims 1-31 of copending Application No. 09/827,882. In particular, the Examiner contends that claims 1 and 10 of the above-captioned application is drawn to identical subject matter of claim 8 of co-pending Application No. 09/827,882. Applicant respectfully traverses and requests reconsideration since the two claim sets appear to be substantially different. Applicant respectfully requests that the Examiner point out with particularity how the claims are identical should this rejection be maintained.

Atty. Dkt. No. 2875.0680001

Claims 2, 3 11, 18, and 23-24 have been provisionally rejected on the grounds of non-statutory obviousness-type double patenting as being unpatentable over claims 2, 3, and 23 of copending Application No. 09/827,882 in view of non-Patent Literature Y.K. Kang, *et al.*, "An Efficient Implementation of Hash Function Processor for IPSEC", Proc. Third Asia-Pacific Conf. ASICs, August 2002 ("Kang"). Applicant respectfully traverses and requests reconsideration. As discussed above, the claims of co-pending Application No. 09/827,882 do not appear to be directed to identical subject matter. Applicant therefore respectfully requests withdrawal of the non-statutory double patenting rejection.

Rejections under 35 U.S.C. § 112

Claims 23-24 have been rejected under 35 U.S.C. § 112 as being unpatentable for describing elements in claims 23-24 that were not disclosed and described in the specification. Specifically, the Examiner contends that the multiplexer used to select the output of the combined adder tree, described in claims 23-24, is missing in the specification.

Applicant respectfully disagrees with the Examiner's allegation. Page 24, lines 3-4 of the specification state: "The overall delay of the unrolled SHA1 rounds now becomes the delay to compute S0 or S1 plus the delay to select between them (using a multiplexer (MUX))." The specification clearly describes the multiplexer called out in claims 23-24. For at least this reason, claims 23-24 are patentable over this rejection. Reconsideration and allowance of dependent claims 23 and 24 are respectfully requested.

Rejections under 35 U.S.C. § 102

Claims 1, 3, 5, 10, 12, 16, and 23-24 have been rejected under 35 U.S.C. § 102(a) as being unpatentable over Kang. Applicant respectfully traverses and requests reconsideration.

The Examiner contends Kang discloses an authentication engine architecture for a SHA1 multi-round authentication algorithm, comprising: a hash engine configured for Hash round logic for an SHA1 authentication algorithm, including adder tree, with critical timing path containing a single carry look-ahead adder (CLA). Applicant respectfully disagrees. Nevertheless, Applicant has amended claims 1 and 10 to recite a combined adder tree that has two parallel outputs. Applicant submits that this claim amendment has been added to more particularly point out the invention without narrowing its scope.

Kang fails to describe a combined adder tree with a timing critical path having a single 32-bit carry look-ahead adder (CLA) and two parallel outputs. Thus, Kang does not disclose or suggest a combined adder tree having two parallel outputs. For at least this reason, independent claims 1 and 10 are patentable over the cited reference. Reconsideration and allowance of independent claims 1 and 10 are respectfully requested.

Claims 3, 5, 12, 16, and 23-24 depend from independent claims 1 and 10. Accordingly, these claims are patentable over Kang for the reasons provide above, in addition to their own unique features. Accordingly, Applicant respectfully requests that the rejection of claims 1, 3, 5, 10, 12, 16, and 23-24 be withdrawn.

Rejections under 35 U.S.C. § 103

Claims 2, 4, 6, 7, and 11 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over Kang. Applicant respectfully traverses and requests reconsideration.

As discussed above with respect to independent claims 1 and 10, Kang does not teach, suggest or disclose the a combined adder tree having two parallel outputs. Therefore, for at least this reason, because each dependent claim incorporates all of the elements of the independent claim from which it depends, as well as additional features, the above arguments apply a fortiori to the dependent claims. Thus, claims 2, 4, 6, and 7 which depend on claim 1, and claim 11, which depends on claim 10 are also patentable over Kang. Reconsideration and allowance of claims 2, 4, 6, 7, and 11 is respectfully requested.

Claims 8-9, 13-15, and 17-22 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over Kang in view of B. Schneier, "Applied Cryptography, Second Edition", John Wiley & Sons, New York, 1996, pp. 436-445 ("Schneier"). Applicant respectfully traverses and requests reconsideration.

Applicant disagrees with many of the allegations made by the Examiner in regard to Schneier. However, because each dependent claim incorporates all of the elements of the independent claim from which it depends, as well as additional features, claims 8-9 which depend on claim 1, and claims 13-15 and 17-22, which depend on claim 10 are patentable over Kang and Schneier. Reconsideration and allowance of claims 8-9, 13-15 and 17-22 is respectfully requested.
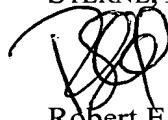
Conclusion

All of the stated grounds of objection and rejection have been properly traversed, accommodated, or rendered moot. Applicant therefore respectfully requests that the Examiner reconsider all presently outstanding objections and rejections and that they be withdrawn. Applicant believes that a full and complete reply has been made to the outstanding Office Action and, as such, the present application is in condition for allowance. If the Examiner believes, for any reason, that personal communication will expedite prosecution of this application, the Examiner is invited to telephone the undersigned at the number provided

Prompt and favorable consideration of this Amendment and Reply is respectfully requested.

Respectfully submitted,

STERNE, KESSLER, GOLDSTEIN & FOX P.L.L.C.

Robert E. Sokohl
Attorney for Applicant
Registration No. 36,013

Date: ___October 10, 2006_____

1100 New York Avenue, N.W.
Washington, D.C. 20005-3934
(202) 371-2600
591744v1

Atty. Dkt. No. 2875.0680001